

UNCLASSIFIED



Internet Explorer 8 STIG

Version: 1.1

Release: 0

26 Apr 2010

STIG.DOD.MIL

Sort Order: [Group ID \(Vulid\), ascending order](#)

Notice: terms-of-use

Description:

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Group ID (Vulid): [V-3427](#)

Group Title: IE - Zones: Use Only Machine Settings

Rule ID: SV-25182r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI320

Rule Title: Internet Explorer is not configured to require consistent security zone settings to all users.

Vulnerability Discussion: This setting enforces consistent security zone settings to all users of the computer. Security zones control browser behavior at various web sites and it is desirable to maintain a consistent policy for all users of a machine.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Security Zones: Use only machine settings" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings Criteria: If the value Security_HKLM_only is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Security Zones: Use only machine settings" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings Criteria: Set the value Security_HKLM_only to REG_DWORD = 1.

Group ID (Vulid): [V-3428](#)

Group Title: IE - Zones: Do Not Allow Users to Change Policies

Rule ID: SV-25181r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI319

Rule Title: Internet Explorer is configured to allow users to change policies.

Vulnerability Discussion: This setting prevents users from changing the Internet Explorer policies on the machine. Policy changes should be made by administrators only, so this setting should be enabled.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet

Explorer “Security Zones: Do not allow users to change policies” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key:
 HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings Criteria: If the value Security_options_edit is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Security Zones: Do not allow users to change policies” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key:
 HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings Criteria: Set the value Security_options_edit to REG_DWORD = 1.

Group ID (Vulid): V-3429

Group Title: IE - Zones: Do Not Allow Users to Add/Delete Sites

Rule ID: SV-25180r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI318

Rule Title: Internet Explorer is configured to allow users to add/delete sites.

Vulnerability Discussion: This setting prevents users from adding sites to various security zones. Users should not be able to add sites to different zones, as this could allow them to bypass security controls of the system.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Security Zones: Do not allow users to add/delete sites” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key:
 HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings Criteria: If the value Security_zones_map_edit is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Security Zones: Do not allow users to add/delete sites” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key:
 HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings Criteria: Set the value Security_zones_map_edit to REG_DWORD = 1.

Group ID (Vulid): V-3430

Group Title: IE - Make Proxy Settings Per Machine

Rule ID: SV-25555r1_rule

Severity: CAT III

Rule Version (STIG-ID): DTBI367

Rule Title: Internet Explorer is not configured to disable making Proxy Settings Per Machine.

Vulnerability Discussion: This setting controls whether or not the Internet Explorer proxy settings are configured on a per-user or per-machine basis.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Make proxy settings per-machine (rather than per user)” to “Disabled”. Procedure: Use the

Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ Criteria: If the value ProxySettingsPerUser is REG_DWORD = 1, this is not a finding.

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Make proxy settings per-machine (rather than per user)” to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ Criteria: Set the value ProxySettingsPerUser to REG_DWORD = 1.

Group ID (Vulid): V-3431

Group Title: IE - Disable Automatic Install of IE Components

Rule ID: SV-28801r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI316

Rule Title: Internet Explorer is configured to allow Automatic Install of components.

Vulnerability Discussion: This setting controls the ability of Internet Explorer to automatically install components if it goes to a site that requires components that are not currently installed. The System Administrator should install all components on the system. If additional components are necessary, the user should inform the SA and have the SA install the components.

Responsibility: System Administrator

IAControls: DCSL-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Disable Automatic Install of Internet Explorer components” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions Criteria: If the value NoJITSetup is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Disable Automatic Install of Internet Explorer components” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions Criteria: Set the value NoJITSetup to REG_DWORD = 1.

Group ID (Vulid): V-3432

Group Title: IE - Disable Periodic Check for IE Updates

Rule ID: SV-25179r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI317

Rule Title: Internet Explorer is configured to automatically check for updates.

Vulnerability Discussion: This setting determines whether or not Internet Explorer will periodically check the Microsoft web sites to determine if there are updates to Internet Explorer available. The SA should manually install all updates on a system so that configuration control is maintained.

Responsibility: System Administrator

IAControls: DCSL-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Disable Periodic Check for Internet Explorer software updates” will be set to “Enabled”. Procedure: Use

the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions Criteria: If the value NoUpdateCheck is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Disable Periodic Check for Internet Explorer software updates" will be set to "Enabled".
Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions Criteria: Set the value NoUpdateCheck to REG_DWORD = 1.

Group ID (Vulid): V-6243

Group Title: DTBI022-Download signed Active X controls-Internet

Rule ID: SV-25613r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI022

Rule Title: The Download signed ActiveX controls property is not set properly for the Internet Zone.

Vulnerability Discussion: Active X controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Download signed ActiveX controls" will be set to "Enabled" and "Disable". **Procedure:** Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1001 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Download signed ActiveX controls" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1001 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6244

Group Title: DTBI023-Download unsigned ActiveX controls-Interne

Rule ID: SV-25615r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI023

Rule Title: The Download unsigned ActiveX controls property is not set properly for the Internet Zone.

Vulnerability Discussion: Active X controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites and they must be digitally signed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Download unsigned ActiveX controls" will be set to "Enabled" and "Disable". **Procedure:** Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value

1004 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Download unsigned ActiveX controls" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1004 to REG_DWORD = 3 (Disabled = 3).

Group ID (Valid): V-6245

Group Title: DTBI024-Initialize and script ActiveX controls

Rule ID: SV-25616r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI024

Rule Title: The Initialize and script ActiveX controls not marked as safe property is not set properly for the Internet Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe scripting should not be executed. Although this is not a complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Initialize and script ActiveX controls not marked as safe" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1201 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Initialize and script ActiveX controls not marked as safe" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1201 is REG_DWORD = 3 (Disabled = 3).

Group ID (Valid): V-6248

Group Title: DTBI030-Font download control - Internet Zone

Rule ID: SV-25609r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI030

Rule Title: The Font download control is not set properly for the Internet Zone.

Vulnerability Discussion: Download of fonts can sometimes contain malicious code.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow font downloads" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1604

is REG_DWORD = 1 (Prompt = 1), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow font downloads" will be set to "Enabled" and "Disable". Change the registry key
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1604 to REG_DWORD = 1 (Prompt = 1).

Group ID (Vulid): V-6249

Group Title: DTBI031-Java Permissions not set for Internet Zone

Rule ID: SV-25618r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI031

Rule Title: The Java Permissions is not set properly for the Internet Zone.

Vulnerability Discussion: Java must have levels of protection based upon the site being browsed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Java permissions" will be set to "Enabled" and "Disable Java". Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1C00 is REG_DWORD = 0 (Disabled = 0), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Java permissions" will be set to "Enabled" and "Disable Java". Change the registry key
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1C00 to REG_DWORD = 0 (Disabled = 0).

Group ID (Vulid): V-6250

Group Title: DTBI032-Access data sources across domains-Interne

Rule ID: SV-25606r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI032

Rule Title: The Access data sources across domains is not set properly for the Internet Zone.

Vulnerability Discussion: Access to data sources across multiple domains must be controlled based upon the site being browsed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Access data sources across domains" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1406 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components ->

Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Access data sources across domains" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1406 to REG_DWORD = 3 (Disabled = 3).

Group ID (Valid): V-6253

Group Title: DTBI036-Drag and drop or copy and paste-Internet

Rule ID: SV-25608r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI036

Rule Title: The Allow Drag and drop or copy and paste files is not set properly for the Internet Zone.

Vulnerability Discussion: Drag and Drop or copy and paste files must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow drag and drop or copy and paste files" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value for 1802 is REG_DWORD = 3 (Disable= 3) or the value does not exist, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow drag and drop or copy and paste files" will be set to "Enabled" and "Disable". If a value for this zone is present and not set to 3, change the registry key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1802 to REG_DWORD = 3 (Disable= 3).

Group ID (Valid): V-6254

Group Title: DTBI037-Installation of desktop items - Internet

Rule ID: SV-25610r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI037

Rule Title: The Installation of desktop items is not set properly for the Internet Zone.

Vulnerability Discussion: Installation of items must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow installation of desktop items" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1800 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow installation of desktop items" will be set to "Enabled" and "Disable". Change the registry key

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1800 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6255

Group Title: DTBI038-Launching programs and files in IFRAME-Int

Rule ID: SV-25619r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI038

Rule Title: The Launching programs and files in IFRAME are not set properly for the Internet Zone.

Vulnerability Discussion: Launching of programs in IFRAME must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Launching applications and files in an IFRAME" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1804 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Launching applications and files in an IFRAME" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1804 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6256

Group Title: DTBI039-Navigate sub-frames across domains-Interne

Rule ID: SV-25624r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI039

Rule Title: The Navigate sub-frames across different domains is not set properly for the Internet Zone.

Vulnerability Discussion: Frames that navigate across different domains are a security concern, because the user may think they are accessing pages on one site while they are actually accessing pages on another site.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Navigate sub-frames across different domains" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1607 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Navigate sub-frames across different domains" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value

1607 to REG_DWORD = 3.

Group ID (Vulid): V-6257

Group Title: DTBI040-Software channel permissions - Internet

Rule ID: SV-25625r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI040

Rule Title: The Software channel permissions is not set properly for the Internet Zone.

Vulnerability Discussion: Software Channel permissions must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Software channel permissions" will be set to "Enabled" and "High: Safety". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1E05 is REG_DWORD = 65536 (High Safety), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Software channel permissions" will be set to "Enabled" and "High: Safety". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1E05 to REG_DWORD = 65536 (High Safety).

Group ID (Vulid): V-6259

Group Title: DTBI042-Userdata persistence - Internet Zone

Rule ID: SV-25626r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI042

Rule Title: The Userdata persistence is not set properly for the Internet Zone.

Vulnerability Discussion: Userdata persistence must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Userdata persistence" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1606 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Userdata persistence" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1606 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6260

Group Title: DTBI044-Allow paste operations via script-Internet

Rule ID: SV-25607r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI044

Rule Title: The Allow paste operations via script is not set properly for the Internet Zone.

Vulnerability Discussion: Allow paste operations via script must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow cut, copy or paste operations from the clipboard via script" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1407 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow cut, copy or paste operations from the clipboard via script" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1407 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6262

Group Title: DTBI046-User Authentication-Logon - Internet Zone

Rule ID: SV-25622r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI046

Rule Title: The user Authentication - Logon is not set properly for the Internet Zone.

Vulnerability Discussion: Care must be taken with user credentials and how automatic logons are performed and how default Windows credentials are passed to web sites.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Logon options" will be set to "Enabled" and "Prompt for user name and password". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1A00 is REG_DWORD = 65536 (decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Logon options" will be set to "Enabled" and "Prompt for user name and password". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1A00 to REG_DWORD = 65536 (decimal).

Group ID (Vulid): V-6267

Group Title: DTBI061-Java Permissions not set - Local Zone

Rule ID: SV-25627r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI061

Rule Title: The Java Permissions is not set properly for the Local Zone.

Vulnerability Discussion: Java must have a level of protection based upon the site being browsed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Intranet Zone -> "Java permissions" will be set to "Enabled" and "High Safety". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1 Criteria: If the value 1C00 is REG_DWORD = 65536, (High Safety), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Intranet Zone -> "Java permissions" will be set to "Enabled" and "High Safety". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1 Criteria: Set the value 1C00 to REG_DWORD = 65536, (High Safety).

Group ID (Vulid): V-6281

Group Title: DTBI091-Java Permissions not set - Trusted Sites

Rule ID: SV-25647r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI091

Rule Title: The Java Permissions is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: Java must have a level of protection based upon the site being browsed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Trusted Sites Zone -> "Java permissions" will be set to "Enabled" and "High Safety". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2 Criteria: If the value 1C00 is REG_DWORD = 65536, (High Safety), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Trusted Sites Zone -> "Java permissions" will be set to "Enabled" and "High Safety". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2 Criteria: Set the value 1C00 to REG_DWORD = 65536, (High Safety).

Group ID (Vulid): V-6289

Group Title: DTBII12-Download signed ActiveX - Restricted Sites

Rule ID: SV-25636r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBII12

Rule Title: The Download signed ActiveX controls property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Download signed ActiveX controls" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1001 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Download signed ActiveX controls" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1001 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6290

Group Title: DTBII13-Download unsigned ActiveX - Restricted Sit

Rule ID: SV-25637r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBII13

Rule Title: The Download unsigned ActiveX controls property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites and they must be digitally signed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Download unsigned ActiveX controls" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1004 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Download unsigned ActiveX controls" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1004 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6291

Group Title: DTBI114-Initialize and script ActiveX - Restricted

Rule ID: SV-25638r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI114

Rule Title: The Initialize and script ActiveX controls not marked as safe property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Initialize and script ActiveX controls not marked as safe" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1201 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Initialize and script ActiveX controls not marked as safe" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1201 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6292

Group Title: DTBI115-Run ActiveX controls and plugins-Restricted

Rule ID: SV-25643r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI115

Rule Title: Run ActiveX controls and plug-ins property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run ActiveX controls and plugins" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1200 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run ActiveX controls and plugins" will be set to "Enabled" and "Disable". Change the registry key

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1200 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6293

Group Title: DTBI116-Script ActiveX controls marked safe-Restri

Rule ID: SV-25644r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI116

Rule Title: The Script ActiveX controls marked safe for scripting property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed.

Although this is not a complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Script ActiveX controls marked safe for scripting" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1405 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Script ActiveX controls marked safe for scripting" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1405 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6294

Group Title: DTBI119-File download control - Restricted Sites

Rule ID: SV-25632r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI119

Rule Title: The File download control is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Files should not be able to be downloaded from sites that are considered restricted.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow file downloads" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1803 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow file downloads"

will be set to “Enabled” and “Disable”. Change the registry key
 HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value
 1803 to REG_DWORD = 3 (Disabled = 3).

Group ID (Valid): V-6295

Group Title: DTBI120-Font download control - Restricted Sites

Rule ID: SV-25633r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI120

Rule Title: The Font download control is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Download of fonts can sometimes contain malicious code. Files should not be downloaded from restricted sites.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Allow font downloads” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1604 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Allow font downloads” will be set to “Enabled” and “Disable”. Change the registry key
 HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1604 to REG_DWORD = 3 (Disabled = 3).

Group ID (Valid): V-6297

Group Title: DTBI122-Access data sources - Restricted Sites

Rule ID: SV-25628r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI122

Rule Title: The Access data sources across domains is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: The restricted zones is used for MS Outlook. This zone must be set properly to ensure Outlook is secured.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Access data sources across domains” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1406 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Access data sources across domains” will be set to “Enabled” and “Disable”. Change the registry key

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1406 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6298

Group Title: DTBI123-Allow META REFRESH - Restricted Sites

Rule ID: SV-25635r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI123

Rule Title: The Allow META REFRESH is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Allow META REFRESH must have a level of protection based upon the site being browsed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow META REFRESH" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1608 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow META REFRESH" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1608 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6301

Group Title: DTBI126-Drag and drop or copy and paste - Restrict

Rule ID: SV-25631r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI126

Rule Title: The Drag and drop or copy and paste files is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Drag and Drop of files must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow drag and drop or copy and paste files" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1802 is REG_DWORD=3 (Disabled), this is not a finding

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow drag and drop or copy and paste files" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1802 to

REG_DWORD=3 (Disabled).

Group ID (Valid): V-6302

Group Title: DTBI127-Installation of desktop items - Restricted

Rule ID: SV-25634r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI127

Rule Title: The Installation of desktop items is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Installation of items must have level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow installation of desktop items" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1800 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow installation of desktop items" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1800 to REG_DWORD = 3 (Disabled = 3).

Group ID (Valid): V-6303

Group Title: DTBI128-Launching programs and files in IFRAME-Res

Rule ID: SV-25640r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI128

Rule Title: The Launching programs and files in IFRAME is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Launching of programs in IFRAME must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Launching applications and files in an IFRAME" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1804 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Launching applications and files in an IFRAME" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1804 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6304

Group Title: DTBI129-Navigate sub-frames across domain - Restrict

Rule ID: SV-25642r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI129

Rule Title: The Navigate windows and frames across different domains are not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Frames that navigate across different domains are a security concern, because users may think they are accessing pages on one site while they are actually accessing pages on another site.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Navigate windows and frames across different domains" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1607 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Navigate windows and frames across different domains" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1607 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6305

Group Title: DTBI130-Software channel permissions - Restricted

Rule ID: SV-25645r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI130

Rule Title: The Software channel permissions is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Software channel permissions must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Software channel permissions" will be set to "Enabled" and "High Safety". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1E05 is REG_DWORD = 65536 (decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Software channel permissions" will be set to "Enabled" and "High Safety". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1E05 to REG_DWORD = 65536 (decimal).

Group ID (Vulid): V-6307

Group Title: DTBI132-Userdata persistence - Restricted Sites

Rule ID: SV-25646r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI132

Rule Title: The Userdata persistence is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: No persistence data should exist and be used in the Restricted Sites Zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Userdata persistence" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1606 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Userdata persistence" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1606 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6308

Group Title: DTBI133-Active scripting - Restricted Sites

Rule ID: SV-25629r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI133

Rule Title: The Active scripting is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Active scripting must have a level of protection based upon the site being accessed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow active scripting" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1400 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow active scripting" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1400 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6309

Group Title: DTBI134-Allow paste operations via scripts-Restrict

Rule ID: SV-25630r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI134

Rule Title: The Allow paste operations via script is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: The Allow paste operations via script must have a level of protection based upon the site being browsed.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow cut, copy or paste operations from the clipboard via script" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1407 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow cut, copy or paste operations from the clipboard via script" will be set to "Enabled" and "Disable". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1407 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6311

Group Title: DTBI136-User Authentication - Logon - Restricted

Rule ID: SV-25641r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI136

Rule Title: The User Authentication – Logon is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Care must be taken with user credentials and how automatic logons are performed and how default Windows credentials are passed to web sites.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Logon options" will be set to "Enabled" and "Anonymous logon". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1A00 is REG_DWORD = 196608 (decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Logon options" will be set to "Enabled" and "Anonymous logon". Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1A00 to REG_DWORD = 196608 (decimal).

Group ID (Vulid): V-7007

Group Title: DTBI121-Java Permissions not set for Restricted

Rule ID: SV-25639r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI121

Rule Title: The Java Permissions is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Java must have a level of protection based upon the site being browsed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Java permissions" will be set to "Enabled" and "Disable Java". Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1C00 is REG_DWORD = 0 (Disabled = 0), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Java permissions" will be set to "Enabled" and "Disable Java". Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1C00 to REG_DWORD = 0 (Disabled = 0).

Group ID (Vulid): V-14245

Group Title: DTBI697 - IE - Users enable or disable add-ons

Rule ID: SV-25817r1_rule

Severity: CAT III

Rule Version (STIG-ID): DTBI697

Rule Title: Internet Explorer - Do not allow users to enable or disable add-ons.

Vulnerability Discussion: This check verifies that the system is configured to allow users to enable or disable add-ons through Add-On Manager in Internet Explorer.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Do Not Allow Users to enable or Disable Add-Ons" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Restrictions Criteria: If the value NoExtensionManagement "does not" exist or the value is set to REG_DWORD = 0, this is not a finding. If the value NoExtensionManagement "does" exist and is set to REG_DWORD = 1 (decimal), this is a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Do Not Allow Users to enable or Disable Add-Ons" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Restrictions Criteria: Remove the value NoExtensionManagement or set to REG_DWORD = 0 (decimal).

Group ID (Vulid): V-15490

Group Title: DTBI305-Automatic configuration is not disabled

Rule ID: SV-25553r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI305

Rule Title: Automatic configuration of Internet Explorer is not disabled.

Vulnerability Discussion: This setting specifies to automatically detect the proxy server settings used to connect to the Internet and customize Internet Explorer. This setting specifies that Internet Explorer use the configuration settings provided in a file by the system administrator. If you enable this policy setting, the user will not be able to do automatic configuration. You can import your current connection settings from your machine using Internet Explorer Maintenance under Admin Templates using group policy editor. If you disable or do not configure this policy setting, the user will have the freedom to automatically configure these settings.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable changing Automatic Configuration settings" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: If the value Autoconfig is REG_DWORD = 1 (Hex), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable changing Automatic Configuration settings" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: Set the value Autoconfig to REG_DWORD = 1 (Hex).

Group ID (Vulid): V-15491

Group Title: DTBI310-Showing the splash screen is not disabled

Rule ID: SV-25554r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI310

Rule Title: Showing the splash screen is not disabled.

Vulnerability Discussion: The Disable showing the splash screen setting prevents the Internet Explorer splash screen from appearing when users start the browser. Enabling this policy causes the splash screen, which normally displays the program name, licensing, and copyright information, to not display. Setting Disable showing the splash screen to disable or Not Configured allows the splash screen to display when users start the browser.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable showing the splash screen" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions Criteria: If the value NoSplash is REG_DWORD = 1 (Hex), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable showing the splash screen" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions Criteria: Set the value NoSplash to REG_DWORD = 1 (Hex).

Group ID (Vulid): V-15492

Group Title: DTBI315 - Prevent participation in the Customer Ex

Rule ID: SV-25556r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI315

Rule Title: Prevent participation in the Customer Experience Improvement Program is not disabled.

Vulnerability Discussion: This setting controls whether users can participate in the Microsoft Customer Experience Improvement Program (CEIP) to help improve Microsoft applications.

When users choose to participate in the CEIP, applications automatically send information to Microsoft about how the applications are used. This information is combined with other CEIP data to help Microsoft solve problems and to improve the products and features customers use most often. This feature does not collect users' names, addresses, or any other identifying information except the IP address that is used to send the data.

By default, users have the opportunity to opt into participation in the CEIP the first time they run an application. If your organization has policies that govern the use of external resources such as the CEIP, allowing users to opt into the program might cause them to violate these policies.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Prevent participation in the Customer Experience Improvement Program" will be set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\SQM Criteria: If the value DisableCustomerImprovementProgram is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Prevent participation in the Customer Experience Improvement Program" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\SQM Criteria: Set the value DisableCustomerImprovementProgram to REG_DWORD = 0.

Group ID (Vulid): V-15494

Group Title: DTBI325 - Turn off the Security Settings Check fea

Rule ID: SV-25560r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI325

Rule Title: Turn off the Security Settings Check feature is not disabled.

Vulnerability Discussion: This policy setting turns off the Security Settings Check feature, which checks Internet Explorer security settings to determine when the settings put Internet Explorer at risk. If you enable this policy setting, the security settings check will not be performed. If you disable or do not configure this policy setting, the security settings check will be performed.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off the Security Settings Check feature" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Security Criteria: If the value DisableSecuritySettingsCheck is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off the Security Settings Check feature" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Security Criteria: Set the value DisableSecuritySettingsCheck to REG_DWORD = 0.

Group ID (Vulid): V-15495

Group Title: DTBI330 - Turn off Managing Phishing filter is not

Rule ID: SV-25559r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI330

Rule Title: Turn off Managing Phishing filter is not disabled.

Vulnerability Discussion: This policy setting allows the user to enable a phishing filter that will warn if the Web site being visited is known for fraudulent attempts to gather personal information through "phishing." If you enable this policy setting, the user will not be prompted to enable the phishing filter. You must specify which mode the phishing filter uses: manual, automatic, or off. If you select manual mode, the phishing filter performs only local analysis and users are prompted to permit any data to be sent to Microsoft. If the feature is fully enabled, all website addresses not contained on the filter's whitelist will be sent automatically to Microsoft without prompting the user. If you disable or do not configure this policy setting, the user will be prompted to decide the mode of operation for the phishing filter.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Managing Phishing filter" will be set to "Enabled" and "Off" selected. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\PhishingFilter Criteria: If the value Enabled is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Managing Phishing filter" will be set to "Enabled" and "Off" selected. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\PhishingFilter Criteria: Set the value Enabled to REG_DWORD = 0.

Group ID (Vulid): V-15497

Group Title: DTBI340 - Allow active content from CDs to run on

Rule ID: SV-25561r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI340

Rule Title: Allow active content from CDs to run on user machines is not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether users receive a dialog requesting permission for active content on a CD to run. If you enable this policy setting, active content on a CD will run without a prompt.

If you disable this policy setting, active content on a CD will always prompt before running. If you do not configure this policy, users can choose whether to be prompted before running active content on a CD.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow active content from CDs to run on user machines" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\Settings Criteria: If the value LOCALMACHINE_CD_UNLOCK is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow active content from CDs to run on user machines" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\Settings Criteria: Set the value LOCALMACHINE_CD_UNLOCK to REG_DWORD = 0.

Group ID (Valid): V-15499

Group Title: DTBI350 - Allow software to run or install even if

Rule ID: SV-25562r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI350

Rule Title: Allow software to run or install even if the signature is invalid is not disabled.

Vulnerability Discussion: Microsoft ActiveX controls and file downloads often have digital signatures attached that vouch for both the file's integrity and the identity of the signer (creator) of the software. An invalid signature might indicate that someone has tampered with the file.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow software to run or install even if the signature is invalid" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Download Criteria: If the value RunInvalidSignatures is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow software to run or install even if the signature is invalid" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Download Criteria: Set the value RunInvalidSignatures to REG_DWORD = 0.

Group ID (Valid): V-15500

Group Title: DTBI355 - Allow third-party browser extensions are

Rule ID: SV-25564r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI355

Rule Title: Allow third-party browser extensions are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer will launch COM add-ons, known as browser helper objects such as toolbars. Browser helper objects may contain flaws such as buffer overruns which impact Internet Explorer's performance or stability. If you enable this policy setting, Internet Explorer automatically launches any browser helper objects that are installed on the user's computer. If you disable this policy setting, browser helper objects do not launch. If you do not configure this policy, Internet Explorer

automatically launches any browser helper objects that are installed on the user's computer.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow third-party browser extensions" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: If the value Enable Browser Extensions is REG_SZ = no, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow third-party browser extensions" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: Set the value Enable Browser Extensions to REG_SZ = no.

Group ID (Vulid): V-15501

Group Title: DTBI360 - Automatically check for Internet Explore

Rule ID: SV-25565r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI360

Rule Title: Automatically check for Internet Explorer updates are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer checks the Internet for newer versions. When Internet Explorer is set to do this, the checks occur approximately every 30 days, and users are prompted to install new versions as they become available. If you enable this policy setting, Internet Explorer checks the Internet for a new version approximately every 30 days and prompts the user to download new versions when they are available. If you disable this policy setting, Internet Explorer does not check the Internet for new versions of the browser, so does not prompt users to install them. If you do not configure this policy setting, Internet Explorer does not check the Internet for new versions of the browser, so does not prompt users to install them.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Automatically check for Internet Explorer updates" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: If the value NoUpdateCheck is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Automatically check for Internet Explorer updates" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: Set the value NoUpdateCheck to REG_DWORD = 1.

Group ID (Vulid): V-15502

Group Title: DTBI365 - Check for server certificate revocation

Rule ID: SV-25566r1_rule

Severity: CAT II**Rule Version (STIG-ID):** DTBI365**Rule Title:** Check for server certificate revocation is not enabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer will check revocation status of servers' certificates. Certificates are revoked when they have been compromised or are no longer valid, and this option protects users from submitting confidential data to a site that may be fraudulent or not secure. If you enable this policy setting, Internet Explorer will check to see if server certificates have been revoked. If you disable this policy setting, Internet Explorer will not check server certificates to see if they have been revoked. If you do not configure this policy setting, Internet Explorer will not check server certificates to see if they have been revoked.

Responsibility: System Administrator**IAControls:** IATS-1**Check Content:**

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Check for server certificate revocation" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings Criteria: If the value CertificateRevocation is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Check for server certificate revocation" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings Criteria: Set the value CertificateRevocation to REG_DWORD = 1.

Group ID (Vulid): V-15503**Group Title:** DTBI370 - Check for signatures on downloaded progr**Rule ID:** SV-25567r1_rule**Severity: CAT II****Rule Version (STIG-ID):** DTBI370**Rule Title:** Check for signatures on downloaded programs is not enabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer checks for digital signatures (which identifies the publisher of signed software and verifies it hasn't been modified or tampered with) on user computers before downloading executable programs. If you enable this policy setting, Internet Explorer will check the digital signatures of executable programs and display their identities before downloading them to user computers.

If you disable this policy setting, Internet Explorer will not check the digital signatures of executable programs or display their identities before downloading them to user computers. If you do not configure this policy, Internet Explorer will not check the digital signatures of executable programs or display their identities before downloading them to user computers.

Responsibility: System Administrator**IAControls:** ECSC-1**Check Content:**

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Check for signatures on downloaded programs" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Download Criteria: If the value CheckExeSignatures is REG_SZ = yes, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components ->

Internet Explorer -> Internet Control Panel -> Advanced Page -> "Check for signatures on downloaded programs" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Download Criteria: Set the value CheckExeSignatures to REG_SZ = yes.

Group ID (Vulid): V-15504

Group Title: DTBI375 - Intranet Sites: Include all network path

Rule ID: SV-25568r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI375

Rule Title: Intranet Sites: Include all network paths (UNCs) are disabled.

Vulnerability Discussion: This policy setting controls whether URLs representing UNC's are mapped into the local Intranet security zone. If you enable this policy setting, all network paths are mapped into the Intranet Zone. If you disable this policy setting, network paths are not necessarily mapped into the Intranet Zone (other rules might map one there). If you do not configure this policy setting, users choose whether network paths are mapped into the Intranet Zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> "Intranet Sites: Include all network paths (UNCs)" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Criteria: If the value UNCAsIntranet is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> "Intranet Sites: Include all network paths (UNCs)" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Criteria: Set the value UNCAsIntranet to REG_DWORD = 0.

Group ID (Vulid): V-15507

Group Title: DTBI385 - Allow script-initiated windows without s

Rule ID: SV-25569r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI385

Rule Title: Allow script-initiated windows without size or position constraints for Internet Zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage restrictions on script-initiated pop-up windows and windows that include the title and status bars.

If you enable this policy setting, Windows Restrictions security will not apply in this zone. The security zone runs without the added layer of security provided by this feature. If you disable this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process. If you do not configure this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow script-initiated windows without size or position constraints" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 2102 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow script-initiated windows without size or position constraints" will be set to "Enabled" and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 2102 to REG_DWORD = 3.

Group ID (Vulid): V-15508

Group Title: DTBI390 - Allow script-initiated windows without s

Rule ID: SV-25585r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI390

Rule Title: Allow script-initiated windows without size or position constraints for Restricted Sites Zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage restrictions on script-initiated pop-up windows and windows that include the title and status bars.

If you enable this policy setting, Windows Restrictions security will not apply in this zone. The security zone runs without the added layer of security provided by this feature. If you disable this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process. If you do not configure this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow script-initiated windows without size or position constraints" will be set to "Enabled" and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2102 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow script-initiated windows without size or position constraints" will be set to "Enabled" and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2102 to REG_DWORD = 3.

Group ID (Vulid): V-15509

Group Title: DTBI395 - Allow Scriptlets are not disabled.

Rule ID: SV-25570r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI395

Rule Title: Allow Scriptlets are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether scriptlets can be allowed.

If you enable this policy setting, users will be able to run scriptlets.

If you disable this policy setting, users will not be able to run scriptlets.

If you do not configure this policy setting, a scriptlet can be enabled or disabled by the user.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow Scriptlets" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1209 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow Scriptlets" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1209 to REG_DWORD = 3.

Group ID (Vulid): V-15513

Group Title: DTBI415 - Automatic prompting for file downloads i

Rule ID: SV-25571r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI415

Rule Title: Automatic prompting for file downloads is not enabled.

Vulnerability Discussion: This policy setting determines whether users will be prompted for non user-initiated file downloads. Regardless of this setting, users will receive file download dialogs for user-initiated downloads. If you enable this setting, users will receive a file download dialog for automatic download attempts.

If you disable or do not configure this setting, file downloads that are not user-initiated will be blocked, and users will see the Information Bar instead of the file download dialog. Users can then click the Information Bar to allow the file download prompt.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Automatic prompting for file downloads" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 2200 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Automatic prompting for file downloads" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 2200 to REG_DWORD = 0.

Group ID (Vulid): V-15515

Group Title: DTBI425 - Java permissions for my computer are not

Rule ID: SV-25578r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI425

Rule Title: Java permissions for my computer are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety. Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Local Machine Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0 Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Local Machine Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0 Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15516

Group Title: DTBI430 - Java permissions for my computer group p

Rule ID: SV-25581r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI430

Rule Title: Java permissions for my computer group policy are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client

computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.

If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.

Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Local Machine Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0 Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Local Machine Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0 Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15517

Group Title: DTBI435 - Java permissions for group policy for lo

Rule ID: SV-25580r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI435

Rule Title: Java permissions for group policy for Local Intranet Zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.

If you enable this policy setting, you can choose options from the drop-down box. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.

If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.

Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Intranet Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1 Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Intranet Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1 Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15518

Group Title: DTBI440 - Java permissions for group policy for tr

Rule ID: SV-25583r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI440

Rule Title: Java permissions for group policy for Trusted Sites Zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.

If you enable this policy setting, you can choose options from the drop-down box. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.

If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.

Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Trusted Sites Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2 Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Trusted Sites Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2 Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15519

Group Title: DTBI445 - Java permissions for group policy for in

Rule ID: SV-25579r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI445

Rule Title: Java permissions for group policy for Internet Zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.

If you enable this policy setting, you can choose options from the drop-down box. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.

If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.

Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3 Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3 Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15520

Group Title: DTBI450 - Java permissions for group policy for re

Rule ID: SV-25582r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI450

Rule Title: Java permissions for group policy for Restricted Sites Zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.

If you enable this policy setting, you can choose options from the drop-down box. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.

If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.

Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Restricted Sites Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4 Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Restricted Sites Zone -> "Java permissions" will be set to "Enabled" and "Disable Java" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following keys: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4 Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15521

Group Title: DTBI455 - Loose or un-compiled XAML files for inte

Rule ID: SV-25572r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI455

Rule Title: Loose XAML files for Internet Zone are not disabled.

Vulnerability Discussion: These are eXtensible Application Markup Language (XAML) files. XAML is an XML-based declarative markup language commonly used for creating rich user interfaces and graphics that leverage the Windows Presentation Foundation. If you enable this policy setting and the dropdown box is set to Enable, XAML files will be automatically loaded inside Internet Explorer. Users will not be able to change this behavior. If the dropdown box is set to Prompt, users will receive a prompt for loading XAML files. If you disable this policy setting, XAML files will not be loaded inside Internet Explorer. Users will not be able to change this behavior. If you do not configure this policy setting, users will have the freedom to decide whether to load XAML files inside Internet Explorer.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Loose XAML files" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 2402 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Loose XAML files" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 2402 to REG_DWORD = 3.

Group ID (Vulid): [V-15522](#)

Group Title: DTBI460 - Loose or un-compiled XAML files for rest

Rule ID: SV-25587r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI460

Rule Title: Loose XAML files for Restricted Sites Zone are not disabled.

Vulnerability Discussion: These are eXtensible Application Markup Language (XAML) files. XAML is an XML-based declarative markup language commonly used for creating rich user interfaces and graphics that leverage the Windows Presentation Foundation. If you enable this policy setting and the dropdown box is set to Enable, XAML files will be automatically loaded inside Internet Explorer. Users will not be able to change this behavior. If the dropdown box is set to Prompt, users will receive a prompt for loading XAML files. If you disable this policy setting, XAML files will not be loaded inside Internet Explorer. Users will not be able to change this behavior. If you do not configure this policy setting, users will have the freedom to decide whether to load XAML files inside Internet Explorer.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Loose XAML files" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2402 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Loose XAML files" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2402 to REG_DWORD = 3.

Group ID (Vulid): V-15523

Group Title: DTBI465 - Open files based on content, not file ex

Rule ID: SV-25573r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI465

Rule Title: Open files based on content, not file extension for Internet Zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage MIME sniffing for file promotion from one type to another based on a MIME sniff. A MIME sniff is the recognition by Internet Explorer of the file type based on a bit signature. If you enable this policy setting, the MIME Sniffing Safety Feature will not apply in this zone. The security zone will run without the added layer of security provided by this feature. If you disable this policy setting, the actions that may be harmful cannot run; this Internet Explorer security feature will be turned on in this zone, as dictated by the feature control setting for the process.

If you do not configure this policy setting, the MIME Sniffing Safety Feature will not apply in this zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Open files based on content, not file extension" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 2100 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Open files based on content, not file extension" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 2100 to REG_DWORD = 3.

Group ID (Vulid): V-15524

Group Title: DTBI470 - Open files based on content, not file ex

Rule ID: SV-25588r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI470

Rule Title: Open files based on content, not file extension for Restricted Sites Zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage MIME sniffing for file promotion from one type to another based on a MIME sniff. A MIME sniff is the recognition by Internet Explorer of the file type based on a bit signature. If you enable this policy setting, the MIME Sniffing Safety Feature will not apply in this zone. The security zone will run without the added layer of security provided by this feature. If you disable this policy setting, the actions that may be harmful cannot run; this Internet Explorer security feature will be turned on in this

zone, as dictated by the feature control setting for the process.

If you do not configure this policy setting, the MIME Sniffing Safety Feature will not apply in this zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Open files based on content, not file extension" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2100 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Open files based on content, not file extension" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2100 to REG_DWORD = 3.

Group ID (Vulid): [V-15525](#)

Group Title: DTBI475 - Turn Off First-Run Opt-In for internet z

Rule ID: SV-25574r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI475

Rule Title: Turn Off First-Run Opt-In for Internet Zone is not disabled.

Vulnerability Discussion: This policy setting controls the First Run response that users see on a zone-by-zone basis. When a user encounters a new control that has not previously run in Internet Explorer, they may be prompted to approve the control. This feature determines if the user gets the prompt or not.

If you enable this policy setting, the Gold Bar prompt will be turned off in the corresponding zone. If you disable this policy setting, the Gold Bar prompt will be turned on in the corresponding zone. If you do not configure this policy setting, the first-run prompt is turned off by default.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Turn Off First-Run Opt-In" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1208 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Turn Off First-Run Opt-In" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1208 to REG_DWORD = 0.

Group ID (Vulid): [V-15526](#)

Group Title: DTBI480 - Turn Off First-Run Opt-In for restricted

Rule ID: SV-25592r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI480

Rule Title: Turn Off First-Run Opt-In for Restricted Sites Zone is not disabled.

Vulnerability Discussion: This policy setting controls the First Run response that users see on a zone-by-zone basis. When a user encounters a new control that has not previously run in Internet Explorer, they may be prompted to approve the control. This feature determines if the user gets the prompt or not.

If you enable this policy setting, the Gold Bar prompt will be turned off in the corresponding zone. If you disable this policy setting, the Gold Bar prompt will be turned on in the corresponding zone. If you do not configure this policy setting, the first-run prompt is turned off by default.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Turn Off First-Run Opt-In" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1208 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Turn Off First-Run Opt-In" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1208 to REG_DWORD = 0.

Group ID (Vulid): [V-15527](#)

Group Title: DTBI485 - Turn on Protected Mode internet zone is

Rule ID: SV-25575r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI485

Rule Title: Turn on Protected Mode Internet Zone is not enabled.

Vulnerability Discussion: Protected mode protects Internet Explorer from exploited vulnerabilities by reducing the locations Internet Explorer can write to in the registry and the file system. If you enable this policy setting, Protected Mode will be turned on. Users will not be able to turn off protected mode. If you disable this policy setting, Protected Mode will be turned off. It will revert to Internet Explorer 6 behavior that allows for Internet Explorer to write to the registry and the file system. Users will not be able to turn on protected mode. If you do not configure this policy, users will be able to turn on or off protected mode. Requires Windows Vista; will be ignored by Windows XP.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Turn on Protected Mode" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 2500 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components ->

Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Turn on Protected Mode" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 2500 to REG_DWORD = 0.

Group ID (Vulid): V-15528

Group Title: DTBI490 - Turn on Protected Mode for restricted si

Rule ID: SV-25593r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI490

Rule Title: Turn on Protected Mode for Restricted Sites Zone is not enabled.

Vulnerability Discussion: VISTA Only

Protected mode protects Internet Explorer from exploited vulnerabilities by reducing the locations Internet Explorer can write to in the registry and the file system. If you enable this policy setting, Protected Mode will be turned on. Users will not be able to turn off protected mode. If you disable this policy setting, Protected Mode will be turned off. It will revert to Internet Explorer 6 behavior that allows for Internet Explorer to write to the registry and the file system. Users will not be able to turn on protected mode. If you do not configure this policy, users will be able to turn on or off protected mode.

Requires Windows Vista; will be ignored by Windows XP.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Turn on Protected Mode" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2500 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Turn on Protected Mode" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2500 to REG_DWORD = 0.

Group ID (Vulid): V-15529

Group Title: DTBI495 - Use Pop-up Blocker for internet zone is

Rule ID: SV-25576r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI495

Rule Title: Use Pop-up Blocker for Internet Zone is not enabled.

Vulnerability Discussion: This policy setting allows you to manage whether unwanted pop-up windows appear. Pop-up windows that are opened when the end user clicks a link are not blocked. If you enable this policy setting, most unwanted pop-up windows are prevented from appearing. If you disable this policy setting, pop-up windows are not prevented from appearing. If you do not configure this policy setting, most unwanted pop-up windows are prevented from appearing.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Use Pop-up Blocker" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 1809 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Use Pop-up Blocker" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1809 to REG_DWORD = 0.

Group ID (Vulid): V-15530

Group Title: DTBI500 - Use Pop-up Blocker for restricted sites

Rule ID: SV-25594r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI500

Rule Title: Use Pop-up Blocker for Restricted Sites Zone is not enabled.

Vulnerability Discussion: This policy setting allows you to manage whether unwanted pop-up windows appear. Pop-up windows that are opened when the end user clicks a link are not blocked. If you enable this policy setting, most unwanted pop-up windows are prevented from appearing. If you disable this policy setting, pop-up windows are not prevented from appearing. If you do not configure this policy setting, most unwanted pop-up windows are prevented from appearing.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Use Pop-up Blocker" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1809 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Use Pop-up Blocker" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1809 to REG_DWORD = 0.

Group ID (Vulid): V-15533

Group Title: DTBI515 - Web sites in less privileged Web content

Rule ID: SV-25577r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI515

Rule Title: Web sites in less privileged Web content zones can navigate into Internet Zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Web sites from less privileged zones, such as Restricted Sites, can navigate into this zone.

If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into,

this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature. If you select Prompt in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur. If you disable this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control. If you do not configure this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Web sites in less privileged Web content zones can navigate into this zone" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 2101 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Web sites in less privileged Web content zones can navigate into this zone" will be set to "Enabled" and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 2101 to REG_DWORD = 3.

Group ID (Vulid): V-15534

Group Title: DTBI520 - Web sites in less privileged Web content

Rule ID: SV-25595r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI520

Rule Title: Web sites in less privileged Web content zones can navigate into Restricted Sites Zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Web sites from less privileged zones, such as Restricted Sites, can navigate into this zone.

If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature. If you select Prompt in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur. If you disable this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control. If you do not configure this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Web sites in less privileged Web content zones can navigate into this zone" will be set to "Enabled" and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2101 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Web sites in less

privileged Web content zones can navigate into this zone" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2101 to REG_DWORD = 3.

Group ID (Vulid): V-15545

Group Title: DTBI575 - Allow binary and script behaviors are no

Rule ID: SV-25584r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI575

Rule Title: Allow binary and script behaviors are not disabled.

Vulnerability Discussion: This policy setting allows you to manage dynamic binary and script behaviors; components that encapsulate specific functionality for HTML elements to which they were attached. If you enable this policy setting, binary and script behaviors are available. If you select Administrator approved in the drop-down box, only behaviors listed in the Admin-approved Behaviors under Binary Behaviors Security Restriction policy are available. If you disable this policy setting, binary and script behaviors are not available unless applications have implemented a custom security manager. If you do not configure this policy setting, binary and script behaviors are available.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow binary and script behaviors" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2000 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow binary and script behaviors" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2000 to REG_DWORD = 3.

Group ID (Vulid): V-15546

Group Title: DTBI580 - Automatic prompting for file downloads i

Rule ID: SV-25586r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI580

Rule Title: Automatic prompting for file downloads is not enabled.

Vulnerability Discussion: This policy setting determines whether users will be prompted for non user-initiated file downloads. Regardless of this setting, users will receive file download dialogs for user-initiated downloads. If you enable this setting, users will receive a file download dialog for automatic download attempts. If you disable or do not configure this setting, file downloads that are not user-initiated will be blocked, and users will see the Information Bar instead of the file download dialog. Users can then click the Information Bar to allow the file download prompt.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Automatic prompting for file downloads" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2200 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Automatic prompting for file downloads" will be set to "Enabled" and "Enable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2200 to REG_DWORD = 0.

Group ID (Vulid): V-15548

Group Title: DTBI590 - Internet Explorer Processes for MIME han

Rule ID: SV-25598r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI590

Rule Title: Internet Explorer Processes for MIME handling is not enabled. (Reserved)

Vulnerability Discussion: Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. The Consistent MIME Handling\Internet Explorer Processes policy setting determines whether Internet Explorer requires that all file-type information provided by Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted. If you enable this policy setting, Internet Explorer examines all received files and enforces consistent MIME data for them. If you disable or do not configure this policy setting, Internet Explorer does not require consistent MIME data for all received files and will use the MIME data provided by the file. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistent and properly labeled helps prevent malicious file downloads from infecting your network. This guide recommends you configure this policy as Enabled for all environments specified in this guide.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING
Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING
Criteria: Set the value (Reserved) to REG_SZ = 1.

Group ID (Vulid): V-15549

Group Title: DTBI595 - Internet Explorer Processes for MIME sni

Rule ID: SV-25601r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI595

Rule Title: Internet Explorer Processes for MIME sniffing is not enabled. (Reserved)

Vulnerability Discussion: MIME sniffing is the process of examining the content of a MIME file to determine its context — whether it is a data file, an executable file, or some other type of file. This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. When set to Enabled, MIME sniffing will never promote a file of one type to a more dangerous file type. Disabling MIME sniffing configures Internet Explorer processes to allow a MIME sniff that promotes a file of one type to a more dangerous file type. For example, promoting a text file to an executable file is a dangerous promotion because any code in the supposed text file would be executed. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistently handled helps prevent malicious file downloads from infecting your network. This guide recommends you configure this policy as Enabled for all environments specified in this guide. Note: This setting works in conjunction with, but does not replace, the Consistent MIME Handling settings.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: Set the value (Reserved) to REG_SZ = 1.

Group ID (Vulid): [V-15550](#)

Group Title: DTBI600 - Internet Explorer Processes for MK proto

Rule ID: SV-25648r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI600

Rule Title: Internet Explorer Processes for MK protocol is not enabled. (Explorer)

Vulnerability Discussion: The MK Protocol Security Restriction policy setting reduces attack surface area by blocking the seldom used MK protocol. Some older Web applications use the MK protocol to retrieve information from compressed files. Setting this policy to Enabled blocks the MK protocol for Windows Explorer and Internet Explorer, which causes resources that use the MK protocol to fail. Disabling this setting allows applications to use the MK protocol API. Because the MK protocol is not widely used, it should be blocked wherever it is not needed. This guide recommends you configure this setting to Enabled to block the MK protocol unless it is specifically needed in your environment. Note: Because resources that use the MK protocol will fail when you deploy this setting, you should ensure that none of your applications use the MK protocol.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to

“Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15551

Group Title: DTBI605 - Internet Explorer Processes for MK proto

Rule ID: SV-25605r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI605

Rule Title: Internet Explorer Processes for MK protocol is not enabled. (IExplore)

Vulnerability Discussion: The MK Protocol Security Restriction policy setting reduces attack surface area by blocking the seldom used MK protocol. Some older Web applications use the MK protocol to retrieve information from compressed files. Setting this policy to Enabled blocks the MK protocol for Windows Explorer and Internet Explorer, which causes resources that use the MK protocol to fail. Disabling this setting allows applications to use the MK protocol API. Because the MK protocol is not widely used, it should be blocked wherever it is not needed. This guide recommends you configure this setting to Enabled to block the MK protocol unless it is specifically needed in your environment. Note: Because resources that use the MK protocol will fail when you deploy this setting, you should ensure that none of your applications use the MK protocol.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15552

Group Title: DTBI610 - Internet Explorer Processes for Zone Ele

Rule ID: SV-25649r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI610

Rule Title: Internet Explorer Processes for Zone Elevation is not enabled. (Reserved)

Vulnerability Discussion: Internet Explorer places restrictions on each Web page it opens that are dependent upon the location of the Web page (such as Internet Zone, Intranet Zone, or Local Machine Zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine Zone, which makes the Local Machine Security Zone a prime target for malicious attackers. If you enable this policy setting, any zone can be protected from zone elevation by Internet Explorer processes. This approach stops content running in one zone from gaining the elevated privileges of another zone. If you disable this policy setting, no zone receives such protection for Internet Explorer processes. Because of the severity and relative frequency of zone elevation attacks, this guide recommends that you configure this setting as Enabled in all environments.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: Set the value (Reserved) to REG_SZ = 1.

Group ID (Vulid): V-15556

Group Title: DTBI630 - Internet Explorer Processes for Download

Rule ID: SV-25653r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI630

Rule Title: Internet Explorer Processes for Download prompt is not enabled. (Reserved)

Vulnerability Discussion: In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on users' hard drives if they click the wrong button and accept the download. If you configure the Restrict File Download\Internet Explorer Processes policy setting to Enabled, file download prompts that are not user-initiated are blocked for Internet Explorer processes. If you configure this policy setting as Disabled, prompting will occur for file downloads that are not user-initiated for Internet Explorer processes. Note: This setting is configured as Enabled in all environments specified in this guide to help prevent attackers from placing arbitrary code on users' computers.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD Criteria: Set the value (Reserved) to

REG_SZ = 1.

Group ID (Vulid): V-15557

Group Title: DTBI635 - Internet Explorer Processes for Download

Rule ID: SV-25654r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI635

Rule Title: Internet Explorer Processes for Download prompt is not enabled. (Explorer)

Vulnerability Discussion: In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on users' hard drives if they click the wrong button and accept the download. If you configure the Restrict File Download\Internet Explorer Processes policy setting to Enabled, file download prompts that are not user-initiated are blocked for Internet Explorer processes. If you configure this policy setting as Disabled, prompting will occur for file downloads that are not user-initiated for Internet Explorer processes. Note: This setting is configured as Enabled in all environments specified in this guide to help prevent attackers from placing arbitrary code on users' computers.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15558

Group Title: DTBI640 - Internet Explorer Processes for Download

Rule ID: SV-25655r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI640

Rule Title: Internet Explorer Processes for Download prompt is not enabled. (IExplore)

Vulnerability Discussion: In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on users' hard drives if they click the wrong button and accept the download. If you configure the Restrict File Download\Internet Explorer Processes policy setting to Enabled, file download prompts that are not user-initiated are blocked for Internet Explorer processes. If you configure this policy setting as Disabled, prompting will occur for file downloads that are not user-initiated for Internet Explorer processes. Note: This setting is configured as Enabled in all environments specified in this guide to help prevent attackers from placing arbitrary code on users' computers.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:
 HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:
 HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15559

Group Title: DTBI645 - Internet Explorer Processes for restrict

Rule ID: SV-25659r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI645

Rule Title: Internet Explorer Processes for restricting pop-up windows is not enabled. (Reserved)

Vulnerability Discussion: Internet Explorer allows scripts to programmatically open, resize, and reposition various types of windows. Often, disreputable Web sites will resize windows to either hide other windows or force you to interact with a window that contains malicious code. The Scripted Window Security Restrictions security feature restricts pop-up windows and prohibits scripts from displaying windows in which the title and status bars are not visible to the user or hide other windows' title and status bars. If you enable the Scripted Window Security Restrictions\Internet Explorer Processes policy setting, pop-up windows and other restrictions apply for Windows Explorer and Internet Explorer processes. If you disable or do not configure this policy setting, scripts can continue to create pop-up windows and windows that hide other windows. Recommend configuring this setting to Enabled to help prevent malicious Web sites from controlling your Internet Explorer windows or fooling users into clicking on the wrong window.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:
 HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:
 HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS Criteria: Set the value (Reserved) is REG_SZ = 1.

Group ID (Vulid): V-15560

Group Title: DTBI650 - Run .NET Framework-reliant components no

Rule ID: SV-25589r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI650

Rule Title: Run .NET Framework-reliant components not signed with Authenticode are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether .NET Framework components that are signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link.

If you enable this policy setting, Internet Explorer will execute signed managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute signed managed components. If you disable this policy setting, Internet Explorer will not execute signed managed components. If you do not configure this policy setting, Internet Explorer will execute signed managed components.

This policy setting allows you to manage whether .NET Framework components that are not signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link.

If you enable this policy setting, Internet Explorer will execute unsigned managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute unsigned managed components. If you disable this policy setting, Internet Explorer will not execute unsigned managed components. If you do not configure this policy setting, Internet Explorer will execute unsigned managed components.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run .NET Framework-reliant components not signed with Authenticode" will be set to "Enabled" and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2004 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run .NET Framework-reliant components not signed with Authenticode" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2004 to REG_DWORD = 3.

Group ID (Vulid): V-15561

Group Title: DTBI655 - Run .NET Framework-reliant components si

Rule ID: SV-25590r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI655

Rule Title: Run .NET Framework-reliant components signed with Authenticode are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether .NET Framework components that are not signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link.

If you enable this policy setting, Internet Explorer will execute unsigned managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute unsigned managed components. If you disable this policy setting, Internet Explorer will not execute unsigned managed components. If you do not configure this policy setting, Internet Explorer will execute unsigned managed components.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run .NET Framework-reliant components signed with Authenticode" will be set to "Enabled" and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2001 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run .NET Framework-reliant components signed with Authenticode" will be set to "Enabled" and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2001 to REG_DWORD = 3.

Group ID (Vulid): V-15562

Group Title: DTBI670 - Scripting of Java applets is not disable

Rule ID: SV-25591r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI670

Rule Title: Scripting of Java applets is not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether applets are exposed to scripts within the zone. If you enable this policy setting, scripts can access applets automatically without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow scripts to access applets. If you disable this policy setting, scripts are prevented from accessing applets. If you do not configure this policy setting, scripts can access applets automatically without user intervention.

Note: This only applies to MS Java, not to Sun Java.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Scripting of Java applets" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1402 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Scripting of Java applets" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1402 to REG_DWORD = 3.

Group ID (Vulid): V-15563

Group Title: DTBI675 - Turn off changing the URL to be displaye

Rule ID: SV-25596r1_rule

Severity: CAT II**Rule Version (STIG-ID):** DTBI675**Rule Title:** Turn off changing the URL to be displayed for checking updates to Internet Explorer and Internet Tools is not disabled.

Vulnerability Discussion: This policy setting allows checking for updates for Internet Explorer from the specified URL, included by default in Internet Explorer. If you enable this policy setting, users will not be able to change the URL to be displayed for checking updates to Internet Explorer and Internet Tools. You must specify the URL to be displayed for checking updates to Internet Explorer and Internet Tools. If you disable or do not configure this policy setting, users will be able to change the URL to be displayed for checking updates to Internet Explorer and Internet Tools.

Responsibility: System Administrator**IAControls:** ECSC-1**Check Content:**

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Component Updates -> Periodic check for updates to Internet Explorer and Internet Tools -> "Turn off changing the URL to be displayed for checking updates to Internet Explorer and Internet Tools" will be set to "Enabled" and "blank or empty" selection box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: The Update_Check_Page value must exist. The value must contain no data value. If the value Update_Check_Page is not present, this is a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Component Updates -> Periodic check for updates to Internet Explorer and Internet Tools -> "Turn off changing the URL to be displayed for checking updates to Internet Explorer and Internet Tools" will be set to "Enabled" and "blank or empty" selection box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: Create the value Update_Check_Page. The value must contain no data.

Group ID (Vulid): [V-15564](#)**Group Title:** DTBI680 - Turn off configuring the update check in**Rule ID:** SV-25597r1_rule**Severity:** CAT II**Rule Version (STIG-ID):** DTBI680**Rule Title:** Turn off configuring the update check interval is not disabled.

Vulnerability Discussion: This setting specifies the update check interval. The default value is 30 days.

If you enable this policy setting, the user will not be able to configure the update check interval. You have to specify the update check interval.

If you disable or do not configure this policy setting, the user will have the freedom to configure the update check interval.

Responsibility: System Administrator**IAControls:** ECSC-1**Check Content:**

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Component Updates -> Periodic check for updates to Internet Explorer and Internet Tools -> "Turn off configuring the update check interval (in days)" will be set to "Enabled" and "30" selected from drop down box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: If the value Update_Check_Interval is REG_DWORD = 30 (Decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components ->

Internet Explorer -> Internet Settings -> Component Updates -> Periodic check for updates to Internet Explorer and Internet Tools -> "Turn off configuring the update check interval (in days)" will be set to "Enabled" and "30" selected from drop down box. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: Set the value Update_Check_Interval to REG_DWORD = 30 (Decimal).

Group ID (Vulid): V-15565

Group Title: DTBI592 - Internet Explorer Processes for MIME han

Rule ID: SV-25599r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI592

Rule Title: Internet Explorer Processes for MIME handling is not enabled. (Explorer)

Vulnerability Discussion: Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. The Consistent MIME Handling\Internet Explorer Processes policy setting determines whether Internet Explorer requires that all file-type information provided by Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted. If you enable this policy setting, Internet Explorer examines all received files and enforces consistent MIME data for them. If you disable or do not configure this policy setting, Internet Explorer does not require consistent MIME data for all received files and will use the MIME data provided by the file. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistent and properly labeled helps prevent malicious file downloads from infecting your network. This guide recommends you configure this policy as Enabled for all environments specified in this guide.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15566

Group Title: DTBI594 - Internet Explorer Processes for MIME han

Rule ID: SV-25600r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI594

Rule Title: Internet Explorer Processes for MIME handling is not enabled. (IExplore)

Vulnerability Discussion: Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. The Consistent MIME Handling\Internet Explorer Processes policy setting determines whether Internet Explorer requires that all file-type information provided by

Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted. If you enable this policy setting, Internet Explorer examines all received files and enforces consistent MIME data for them. If you disable or do not configure this policy setting, Internet Explorer does not require consistent MIME data for all received files and will use the MIME data provided by the file. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistent and properly labeled helps prevent malicious file downloads from infecting your network. This guide recommends you configure this policy as Enabled for all environments specified in this guide.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15568

Group Title: DTBI599 - Internet Explorer Processes for MK proto

Rule ID: SV-25604r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI599

Rule Title: Internet Explorer Processes for MK protocol is not enabled. (Reserved)

Vulnerability Discussion: The MK Protocol Security Restriction policy setting reduces attack surface area by blocking the seldom used MK protocol. Some older Web applications use the MK protocol to retrieve information from compressed files. Setting this policy to Enabled blocks the MK protocol for Windows Explorer and Internet Explorer, which causes resources that use the MK protocol to fail. Disabling this setting allows applications to use the MK protocol API. Because the MK protocol is not widely used, it should be blocked wherever it is not needed. This guide recommends you configure this setting to Enabled to block the MK protocol unless you specifically need it in your environment. Note: Because resources that use the MK protocol will fail when you deploy this setting, you should ensure that none of your applications use the MK protocol.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL Criteria: Set the value (Reserved) to REG_SZ = 1.

Group ID (Vulid): V-15569

Group Title: DTBI612 - Internet Explorer Processes for Zone Ele

Rule ID: SV-25650r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI612

Rule Title: Internet Explorer Processes for Zone Elevation is not enabled. (Explorer)

Vulnerability Discussion: Internet Explorer places restrictions on each Web page it opens that are dependent upon the location of the Web page (such as Internet Zone, Intranet Zone, or Local Machine Zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine Zone, which makes the Local Machine Security Zone a prime target for malicious attackers. If you enable this policy setting, any zone can be protected from zone elevation by Internet Explorer processes. This approach stops content running in one zone from gaining the elevated privileges of another zone. If you disable this policy setting, no zone receives such protection for Internet Explorer processes. Because of the severity and relative frequency of zone elevation attacks, this guide recommends that you configure this setting as Enabled in all environments.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION
Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION
Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15570

Group Title: DTBI614 - Internet Explorer Processes for Zone Ele

Rule ID: SV-25651r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI614

Rule Title: Internet Explorer Processes for Zone Elevation is not enabled. (IExplore)

Vulnerability Discussion: Internet Explorer places restrictions on each Web page it opens that are dependent upon the location of the Web page (such as Internet Zone, Intranet Zone, or Local Machine Zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine Zone, which makes the Local Machine Security Zone a prime target for malicious attackers. If you enable this policy setting, any zone can be protected from zone elevation by Internet Explorer processes. This approach stops content running in one zone from gaining the elevated privileges of another zone. If you disable this policy setting, no zone receives such protection for Internet Explorer processes. Because of the severity and relative frequency of zone elevation attacks, this guide recommends that you configure this setting as Enabled in all environments.

Responsibility: System Administrator

IAControls: ECSC-1**Check Content:**

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15571

Group Title: DTBI647 - Internet Explorer Processes for restrict

Rule ID: SV-25661r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI647

Rule Title: Internet Explorer Processes for restricting pop-up windows is not enabled. (Explorer)

Vulnerability Discussion: Internet Explorer allows scripts to programmatically open, resize, and reposition various types of windows. Often, disreputable Web sites will resize windows to either hide other windows or force you to interact with a window that contains malicious code. The Scripted Window Security Restrictions security feature restricts pop-up windows and prohibits scripts from displaying windows in which the title and status bars are not visible to the user or hide other windows' title and status bars. If you enable the Scripted Window Security Restrictions\Internet Explorer Processes policy setting, pop-up windows and other restrictions apply for Windows Explorer and Internet Explorer processes. If you disable or do not configure this policy setting, scripts can continue to create pop-up windows and windows that hide other windows. This guide recommends you configure this setting to Enabled to help prevent malicious Web sites from controlling your Internet Explorer windows or fooling users into clicking on the wrong window.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15572

Group Title: DTBI649 - Internet Explorer Processes for restrict

Rule ID: SV-25663r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI649

Rule Title: Internet Explorer Processes for restricting pop-up windows is not enabled. (IExplorer)

Vulnerability Discussion: Internet Explorer allows scripts to programmatically open, resize, and reposition various types of windows. Often, disreputable Web sites will resize windows to either hide other windows or force you to interact with a window that contains malicious code. The Scripted Window Security Restrictions security feature restricts pop-up windows and prohibits scripts from displaying windows in which the title and status bars are not visible to the user or hide other windows' title and status bars. If you enable the Scripted Window Security Restrictions\Internet Explorer Processes policy setting, pop-up windows and other restrictions apply for Windows Explorer and Internet Explorer processes. If you disable or do not configure this policy setting, scripts can continue to create pop-up windows and windows that hide other windows. This guide recommends you configure this setting to Enabled to help prevent malicious Web sites from controlling your Internet Explorer windows or fooling users into clicking on the wrong window.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15573

Group Title: DTBI685 - Configure Outlook Express is not disable

Rule ID: SV-25665r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI685

Rule Title: Configure Outlook Express is not disabled.

Vulnerability Discussion: The Configure Outlook Express setting allows administrators to enable and disable the ability for Microsoft Outlook® Express users to save or open attachments that can potentially contain a virus. Selecting the block attachments option of this setting prevents users opening or saving attachments to e-mails that could potentially contain a virus.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Configure Outlook Express" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Microsoft\Outlook Express Criteria: If the value BlockExeAttachments is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components ->

Internet Explorer -> "Configure Outlook Express" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Microsoft\Outlook Express Criteria:Set the value BlockExeAttachments to REG_DWORD = 0.

Group ID (Vulid): V-15574

Group Title: DTBI690 - Disable AutoComplete for forms is not en

Rule ID: SV-25666r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI690

Rule Title: Disable AutoComplete for forms is not enabled.

Vulnerability Discussion: This AutoComplete feature suggests possible matches when users are filling up forms. If you enable this setting, the user is not suggested matches when filling forms. The user cannot change it. If you disable this setting, the user is suggested possible matches when filling forms. The user cannot change it. If you do not configure this setting, the user has the freedom to turn on the auto-complete feature for forms. To display this option, the users open the Internet Options dialog box, click the Contents Tab and click the Settings button.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable AutoComplete for forms" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Explorer\Main Criteria: If the value Use FormSuggest is REG_SZ = no, this is not a finding. HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: If the value FormSuggest is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable AutoComplete for forms" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Explorer\Main Criteria: Set the value Use FormSuggest to REG_SZ = no. HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: Set the value FormSuggest to REG_DWORD = 1.

Group ID (Vulid): V-15575

Group Title: DTBI695 - Disable external branding of Internet Ex

Rule ID: SV-25667r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI695

Rule Title: Disable external branding of Internet Explorer is not enabled.

Vulnerability Discussion: Prevents branding of Internet programs, such as customization of Internet Explorer and Outlook Express logos and title bars, by another party. If you enable this policy, it prevents customization of the browser by another party, such as an Internet service provider or Internet content provider. If you disable this policy or do not configure it, users could install customizations from another party-for example, when signing up for Internet services. This policy is intended for administrators who want to maintain a consistent browser across an organization.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable external branding of Internet Explorer" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions Criteria: If the value NoExternalBranding is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable external branding of Internet Explorer" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions Criteria: Set the value NoExternalBranding to REG_DWORD = 1.

Group ID (Vulid): V-15577

Group Title: DTBI705 - Disable the Reset Web Settings feature i

Rule ID: SV-25668r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI705

Rule Title: Disable the Reset Web Settings feature is not enabled.

Vulnerability Discussion: Prevents users from restoring default settings for home and search pages. If you enable this policy, the Reset Web Settings button on the Programs tab in the Internet Options dialog box appears dimmed. If you disable this policy or do not configure it, users can restore the default settings for home and search pages. The "Disable the Programs page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable the Reset Web Settings feature" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: If the value ResetWebSettings is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable the Reset Web Settings feature" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: Set the value ResetWebSettings to REG_DWORD = 1.

Group ID (Vulid): V-15579

Group Title: DTBI715 - Turn off Crash Detection is not enabled.

Rule ID: SV-25558r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI715

Rule Title: Turn off Crash Detection is not enabled.

Vulnerability Discussion: The Turn off Crash Detection policy setting allows you to manage the crash detection feature of add-on management in Internet Explorer. If you enable this policy setting, a crash in Internet Explorer will be similar to one on a computer running Windows XP Professional Service Pack 1 and earlier: Windows Error Reporting will be invoked. If you disable this policy setting, the crash detection feature in add-on management will be functional. Because Internet Explorer crash report information could contain sensitive information from the computer's memory, this guide recommends you configure this option to Enabled unless you are experiencing frequent repeated crashes and need to report them for follow-up troubleshooting. In those cases, you could

temporarily configure the setting to Disabled.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Crash Detection" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Restrictions Criteria: If the value NoCrashDetection is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Crash Detection" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Restrictions Criteria: Set the value NoCrashDetection to REG_DWORD = 1.

Group ID (Vulid): V-15580

Group Title: DTBI720 - Turn off page transitions is not enabled

Rule ID: SV-25671r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI720

Rule Title: Turn off page transitions is not enabled.

Vulnerability Discussion: This policy setting specifies if, as you move from one Web page to another, Internet Explorer fades out of the page you are leaving and fades into the page to which you are going. If you enable this policy setting, page transitions will be turned off. The user cannot change this behavior. If you disable this policy setting, page transitions will be turned on. The user cannot change this behavior. If you do not configure this policy setting, the user can turn on or off page transitions.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Advanced Settings -> Browsing -> "Turn off page transitions" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Explorer\Main Criteria: If the value Page_Transitions is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Advanced Settings -> Browsing -> "Turn off page transitions" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Explorer\Main Criteria: Set the value Page_Transitions to REG_DWORD = 0.

Group ID (Vulid): V-15581

Group Title: DTBI725 - Turn on the auto-complete feature for us

Rule ID: SV-25670r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI725

Rule Title: Turn on the auto-complete feature for user names and passwords on forms are not disabled.

Vulnerability Discussion: This AutoComplete feature can remember and suggest User names and passwords on

Forms. If you enable this setting, the user cannot change "User name and passwords on forms" or "prompt me to save passwords". The Auto Complete feature for User names and passwords on Forms will be turned on. You have to decide whether to select "prompt me to save passwords". If you disable this setting, the user cannot change "User name and passwords on forms" or "prompt me to save passwords". The Auto Complete feature for User names and passwords on Forms is turned off. The user also cannot opt to be prompted to save passwords. If you do not configure this setting, the user has the freedom of turning on Auto complete for User name and passwords on forms and the option of prompting to save passwords. To display this option, the users open the Internet Options dialog box, click the Contents Tab and click the Settings button.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn on the auto-complete feature for user names and passwords on forms" will be set to "Disabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Main Criteria: If the value FormSuggest Passwords is REG_SZ = no, this is not a finding. HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: If the value FormSuggest Passwords is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn on the auto-complete feature for user names and passwords on forms" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Main Criteria: Set the value FormSuggest Passwords to REG_SZ = no. HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: Set the value FormSuggest Passwords to REG_DWORD = 1.

Group ID (Vulid): V-15582

Group Title: DTBI730 - Turn on the Internet Connection Wizard A

Rule ID: SV-25672r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI730

Rule Title: Turn on the Internet Connection Wizard Auto Detect is not disabled.

Vulnerability Discussion: This policy setting determines if the Internet Connection Wizard was completed. If it was not completed, it launches the Internet Connection Wizard. If you enable this policy setting, the Internet Connection Wizard is launched automatically if it was not completed before. The user cannot prevent the wizard from launching. If you disable this policy setting, the Internet Connection Wizard is not launched automatically. The user can launch the wizard manually. If you do not configure this policy setting, the user will have the freedom to decide whether the Internet Connection Wizard should be launched automatically.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Advanced Settings -> Internet Connection -> "Turn on the Internet Connection Wizard Auto Detect" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Connection Wizard Criteria: If the value DisableICW is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Advanced Settings -> Internet Connection -> "Turn on the Internet Connection Wizard Auto Detect" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Policies\Microsoft\Internet Connection Wizard Criteria: Set the value DisableICW to REG_DWORD = 1.

Group ID (Vulid): V-15603

Group Title: DTBI596 - IE Processes for MIME sniffing is n

Rule ID: SV-25602r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI596

Rule Title: Internet Explorer Processes for MIME sniffing is not enabled. (Explorer)

Vulnerability Discussion: MIME sniffing is the process of examining the content of a MIME file to determine its context — whether it is a data file, an executable file, or some other type of file. This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. When set to Enabled, MIME sniffing will never promote a file of one type to a more dangerous file type. Disabling MIME sniffing configures Internet Explorer processes to allow a MIME sniff that promotes a file of one type to a more dangerous file type. For example, promoting a text file to an executable file is a dangerous promotion because any code in the supposed text file would be executed. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistently handled helps prevent malicious file downloads from infecting your network. This guide recommends you configure this policy as Enabled for all environments specified in this guide. Note: This setting works in conjunction with, but does not replace, the Consistent MIME handling settings.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15604

Group Title: DTBI597 - Internet Explorer Processes for MIME sni

Rule ID: SV-25603r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI597

Rule Title: Internet Explorer Processes for MIME sniffing is not enabled. (IExplore)

Vulnerability Discussion: MIME sniffing is the process of examining the content of a MIME file to determine its context — whether it is a data file, an executable file, or some other type of file. This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. When set to Enabled, MIME sniffing will never promote a file of one type to a more dangerous file type. Disabling MIME sniffing configures Internet Explorer processes to allow a MIME sniff that promotes a file of one type to a more dangerous file type. For example, promoting a text file to an executable file is a dangerous promotion because any code in the supposed text file would be executed. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistently handled helps prevent malicious file downloads from infecting your network. This guide recommends you configure this policy as Enabled for all environments specified

in this guide. Note: This setting works in conjunction with, but does not replace, the Consistent MIME handling settings.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to "Enabled". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-16879

Group Title: DTBI025 - The Download signed ActiveX controls pro

Rule ID: SV-26346r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI025

Rule Title: The Download signed ActiveX controls property is not set properly for the Lockdown Zone.

Vulnerability Discussion: This policy setting allows you to manage whether users may download signed ActiveX controls from a page in the zone. If you enable this policy, users can download signed controls without user intervention. If you select Prompt in the drop-down box, users are queried whether to download controls signed by publishers who aren't trusted. Code signed by trusted publishers is silently downloaded. If you disable the policy setting, signed controls cannot be downloaded. If you do not configure this policy setting, users are queried whether to download controls signed by publishers who aren't trusted. Code signed by trusted publishers is silently downloaded.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Download signed ActiveX controls" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3 Criteria: If the value 1001 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Download signed ActiveX controls" will be set to "Enabled" and "Disable" selected from down drop box. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3 Criteria: Set the value 1001 to REG_DWORD = 3.

Group ID (Vulid): V-17296

Group Title: Prevent performance of First Run Customize setting

Rule ID: SV-25824r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI010

Rule Title: Prevent performance of First Run Customize settings is not enabled.

Vulnerability Discussion: This policy setting prevents performance of the First Run Customize settings ability and controls what the user will see when they launch Internet Explorer for the first time after installation of Internet Explorer.

If you enable this policy setting, users must make one of two choices:

- 1: Skip Customize Settings, and go directly to the user's home page.
- 2: Skip Customize Settings, and go directly to the "Welcome to Internet Explorer" Web page.

If you disable or do not configure this policy setting, users go through the regular first run process.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Prevent performance of First Run Customize settings" will be set to "Enabled" and "Go directly to home page" selected. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: If the value DisableFirstRunCustomize is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Prevent performance of First Run Customize settings" will be set to "Enabled" and "Go directly to home page" selected. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Main Criteria: Set the value DisableFirstRunCustomize to REG_DWORD = 1.

Group ID (Vulid): [V-21887](#)

Group Title: History setting is not enabled or set to 40 days.

Rule ID: SV-25652r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI300

Rule Title: Disable Configuring History - History setting is not set to 40 days.

Vulnerability Discussion: This setting specifies the number of days that Internet Explorer keeps track of the pages viewed in the History List. The delete Browsing History option can be accessed using Tools, Internet Options, General tab, and then click Settings under Browsing History. If you enable this policy setting, a user cannot set the number of days that Internet Explorer keeps track of the pages viewed in the History List. You must specify the number of days that Internet Explorer keeps track of the pages viewed in the History List. Users will not be able to delete browsing history. If you disable or do not configure this policy setting, a user can set the number of days that Internet Explorer tracks views of pages in the History List. Users can delete browsing history.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Delete Browsing History -> "Disable "Configuring History" " will be set to "Enabled" and "40" entered in 'Days to keep pages in History'. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: If the value History is REG_DWORD = 1, this is not a finding. HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Url History Criteria: If the value DaysToKeep is REG_DWORD = 40 (decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Delete Browsing History -> "Disable "Configuring History" " will be set to "Enabled" and "40" entered in 'Days to keep pages in History'. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Control Panel Criteria: Set the value History to REG_DWORD = 1 and HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Url History Criteria: Set the value DaysToKeep to REG_DWORD = 40 (decimal).

Group ID (Vulid): V-22108

Group Title: DTBI740: Turn off Managing SmartScreen Filter

Rule ID: SV-25697r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI740

Rule Title: Turn off Managing SmartScreen Filter property is not properly set.

Vulnerability Discussion: This setting allows users to enable the SmartScreen Filter, which then warns if a Web site being visited is known for fraudulent attempts to gather personal information through "phishing" or is known to host malware.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Managing SmartScreen Filter" will be set to "Enabled" and "Off". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\PhishingFilter Criteria: If the value EnabledV8 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Managing SmartScreen Filter" will be set to "Enabled" and "Off". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\PhishingFilter Criteria: Set the value EnabledV8 to REG_DWORD = 0.

Group ID (Vulid): V-22147

Group Title: DTBI750: Include updated Web site lists fm Micro

Rule ID: SV-25699r1_rule

Severity: CAT III

Rule Version (STIG-ID): DTBI750

Rule Title: Include updated Web site lists from Microsoft is not disabled.

Vulnerability Discussion: This policy controls the Web site compatibility lists provided by Microsoft. If you do not configure this setting, the Microsoft Web site list will not be active. The user can enable the functionality using the Compatibility View Settings dialog box.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Compatibility View -> "Include updated Web site lists from Microsoft" will be set to "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\BrowserEmulation Criteria: If the value MSCompatibilityMode is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Compatibility View -> “Include updated Web site lists from Microsoft” will be set to “Disabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\BrowserEmulation Criteria: Set the value MSCompatibilityMode to REG_DWORD = 0.

Group ID (Vulid): V-22148

Group Title: DTBI760: Configure Delete Browsing History on exit

Rule ID: SV-25701r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI760

Rule Title: Configure Delete Browsing History on exit is not disabled.

Vulnerability Discussion: Delete Browsing History on exit automatically deletes specified items when the last browser window closes. Disabling this function will prevent users from deleting their browsing history, which could be used to identify malicious Web sites and files that could later be used for anti-virus and intrusion detection system (IDS) signatures. Furthermore, preventing users from deleting browsing history could be used to identify abusive web surfing on government systems.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Delete Browsing History -> “Configure Delete Browsing History on exit” will be set to “Disabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Privacy Criteria: If the value ClearBrowsingHistoryOnExit is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Delete Browsing History -> “Configure Delete Browsing History on exit” will be set to “Disabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Privacy Criteria: Set the value ClearBrowsingHistoryOnExit to REG_DWORD = 0.

Group ID (Vulid): V-22149

Group Title: DTBI770: Prevent Deleting Web sites that the User

Rule ID: SV-25703r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI770

Rule Title: Prevent Deleting Web sites that the User has Visited is not enabled.

Vulnerability Discussion: This policy prevents users from deleting the history of Web sites the user has visited. If you do not configure this policy setting, the user will be able to select whether to delete or preserve Web sites the user visited when the user clicks Delete.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Delete Browsing History -> “Prevent Deleting Web sites that the User has Visited” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Privacy
Criteria: If the value CleanHistory is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Delete Browsing History -> “Prevent Deleting Web sites that the User has Visited” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Privacy
Criteria: Set the value CleanHistory to REG_DWORD = 0.

Group ID (Vulid): V-22150

Group Title: DTBI780: Turn off InPrivate Browsing

Rule ID: SV-25705r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI780

Rule Title: Turn off InPrivate Browsing is not enabled.

Vulnerability Discussion: InPrivate Browsing lets you control whether or not Internet Explorer 8 saves your browsing history, cookies, and other data. The InPrivate Browsing feature in Internet Explorer 8 makes browser privacy easy by not storing history, cookies, temporary Internet files, or other data. If you do not configure this setting, InPrivate Browsing can be turned on or off through the registry.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> InPrivate -> “Turn off InPrivate Browsing” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Privacy
Criteria: If the value EnableInPrivateBrowsing is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> InPrivate -> “Turn off InPrivate Browsing” will be set to “Enabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Internet Explorer\Privacy
Criteria: Set the value EnableInPrivateBrowsing to REG_DWORD = 0.

Group ID (Vulid): V-22152

Group Title: DTBI800: Allow scripting of IE web browser

Rule ID: SV-25709r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI800

Rule Title: Allow scripting of Internet Explorer web browser control property is not properly set (Internet Zone).

Vulnerability Discussion: This policy setting controls whether a page may control embedded WebBrowser Controls via script. If you do not configure this policy setting, script access to the WebBrowser Control can be enabled or disabled by the user. By default, script access to the WebBrowser control is only allowed in the Local Machine and Intranet Zones.

Responsibility: System Administrator

IAControls: ECSC-1**Check Content:**

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> “Allow scripting of Internet Explorer web browser control” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Criteria: If the value 1206 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> “Allow scripting of Internet Explorer web browser control” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Criteria: Set the value 1206 to REG_DWORD = 3.

Group ID (Valid): V-22153

Group Title: DTBI810: Include local directory path when upload

Rule ID: SV-25711r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI810

Rule Title: Include local directory path when uploading files to a server property is not properly set.

Vulnerability Discussion: This policy setting controls whether or not the local path information will be sent when uploading a file via a HTML form. If the local path information is sent, some information may be unintentionally revealed to the server. If you do not configure this policy setting, the user can choose whether path information will be sent when uploading a file via a form. By default, path information will be sent.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> “Include local directory path when uploading files to a server” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Criteria: If the value 160A is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> “Include local directory path when uploading files to a server” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Criteria: Set the value 160A to REG_DWORD = 3.

Group ID (Valid): V-22154

Group Title: DTBI820: Launching programs and unsafe files prop

Rule ID: SV-25713r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI820

Rule Title: Launching programs and unsafe files property is not properly set (Internet Zone).

Vulnerability Discussion: This policy setting controls whether or not the “Open File – Security Warning” prompt

is shown when launching executables or other unsafe files. If you do not configure this policy setting, users can configure the prompt behavior. By default, execution is blocked in the Restricted Zone, enabled in the Intranet and Local Computer Zone, and set to prompt in the Internet and Trusted Zones.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Launching programs and unsafe files" will be set to "Enabled" and "Prompt". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Criteria: If the value 1806 is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Launching programs and unsafe files" will be set to "Enabled" and "Prompt". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 1806 to REG_DWORD = 1.

Group ID (Vulid): V-22155

Group Title: DTBI830: Only allow approved domains to use Active

Rule ID: SV-25715r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI830

Rule Title: Only allow approved domains to use ActiveX controls without prompt property is not properly set (Internet Zone).

Vulnerability Discussion: This policy setting controls whether or not the user is prompted to allow ActiveX controls to run on Web sites other than the Web site that installed the ActiveX control.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Only allow approved domains to use ActiveX controls without prompt" will be set to "Enabled" and "Enable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Criteria: If the value 120B is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Only allow approved domains to use ActiveX controls without prompt" will be set to "Enabled" and "Enable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 120B to REG_DWORD = 3.

Group ID (Vulid): V-22156

Group Title: DTBI840: Turn on Cross-Site Scripting (XSS) Filter

Rule ID: SV-25717r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI840

Rule Title: Turn on Cross-Site Scripting (XSS) Filter property is not properly set (Internet Zone).

Vulnerability Discussion: The Cross-Site Scripting (XSS) Filter is designed to prevent users from becoming victims of unintentional information disclosure. This setting controls if the Cross-Site Scripting (XSS) Filter detects and prevents cross-site script injection into Web sites in this zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> “Turn on Cross-Site Scripting (XSS) Filter” will be set to “Enabled” and “Enable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Criteria: If the value 1409 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> “Turn on Cross-Site Scripting (XSS) Filter” will be set to “Enabled” and “Enable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Criteria: Set the value 1409 to REG_DWORD = 0.

Group ID (Vulid): V-22157

Group Title: DTBI850: Allow scripting of IE web browser control

Rule ID: SV-25719r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI850

Rule Title: Allow scripting of Internet Explorer web browser control property is not properly configured (Restricted Sites Zone).

Vulnerability Discussion: This policy setting controls whether a page may control embedded WebBrowser Controls via script. If you do not configure this policy setting, script access to the WebBrowser Control can be enabled or disabled by the user. By default, script access to the WebBrowser Control is only allowed in the Local Machine and Intranet Zones.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Allow scripting of Internet Explorer web browser control” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
Criteria: If the value 1206 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Allow scripting of Internet Explorer web browser control” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
Criteria: Set the value 1206 to REG_DWORD = 3.

Group ID (Vulid): V-22158

Group Title: DTBI860: Include local directory path when upload

Rule ID: SV-25721r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI860

Rule Title: Include local directory path when uploading files to a server is not properly set (Restricted Sites Zone).

Vulnerability Discussion: This policy setting controls whether or not the local path information will be sent when uploading a file via a HTML form. If the local path information is sent, some information may be unintentionally revealed to the server. If you do not configure this policy setting, the user can choose whether path information will be sent when uploading a file via a form. By default, path information will be sent.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Include local directory path when uploading files to a server" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 160A is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Include local directory path when uploading files to a server" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 160A to REG_DWORD = 3.

Group ID (Vulid): V-22159

Group Title: DTBI870: Launching programs and unsafe files

Rule ID: SV-25723r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI870

Rule Title: Launching programs and unsafe files property is not properly set (Restricted Sites Zone).

Vulnerability Discussion: This policy setting controls whether or not the "Open File – Security Warning" prompt is shown when launching executables or other unsafe files. If you do not configure this policy setting, users can configure the prompt behavior. By default, execution is blocked in the Restricted Zone, enabled in the Intranet and Local Computer Zones, and set to prompt in the Internet and Trusted Zones.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Launching programs and unsafe files" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1806 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Launching programs and unsafe files" will be set to "Enabled" and "Disable". Procedure: Use the Windows Registry Editor to navigate to the

following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1806 to REG_DWORD = 3.

Group ID (Valid): V-22160

Group Title: DTBI880: Only allow approved domains to use Active

Rule ID: SV-25725r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI880

Rule Title: Only allow approved domains to use ActiveX controls without prompt property is not properly set (Restricted Sites Zone).

Vulnerability Discussion: This policy setting controls whether or not the user is prompted to allow ActiveX controls to run on Web sites other than the Web site that installed the ActiveX control.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Only allow approved domains to use ActiveX controls without prompt” will be set to “Enabled” and “Enable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 120B is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Only allow approved domains to use ActiveX controls without prompt” will be set to “Enabled” and “Enable”. Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 120B to REG_DWORD = 3.

Group ID (Valid): V-22161

Group Title: DTBI890: Turn on Cross-Site Scripting (XSS) Filter

Rule ID: SV-25727r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI890

Rule Title: Turn on Cross-Site Scripting (XSS) Filter property is not properly set (Restricted Sites Zone).

Vulnerability Discussion: This setting controls if the Cross-Site Scripting (XSS) Filter detects and prevents cross-site script injection into Web sites in this zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Turn on Cross-Site Scripting (XSS) Filter” will be set to “Enabled” and “Enable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1409 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components ->

Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> “Turn on Cross-Site Scripting (XSS) Filter” will be set to “Enabled” and “Enable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1409 to REG_DWORD = 0.

Group ID (Vulid): V-22171

Group Title: DTBI900: IE Processes Restrict ActiveX Install

Rule ID: SV-25809r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI900

Rule Title: Internet Explorer Processes Restrict ActiveX Install (Reserved) property is not properly set.

Vulnerability Discussion: This policy setting enables blocking of ActiveX control installation prompts for Internet Explorer processes. If you do not configure this policy setting, the user’s preference will be used to determine whether to block ActiveX control installations for Internet Explorer processes.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict ActiveX Install -> “Internet Explorer Processes” will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict ActiveX Install -> “Internet Explorer Processes” will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL Criteria: Set the value (Reserved) to REG_SZ = 1.

Group ID (Vulid): V-22634

Group Title: DTBI910: Allow status bar updates via script

Rule ID: SV-26380r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI910

Rule Title: Allow status bar updates via script (Internet Zone) property is not properly set.

Vulnerability Discussion: This policy setting allows you to manage whether script is allowed to update the status bar within the zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone “Allow status bar updates via script” will be

set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 2103 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone “Allow status bar updates via script” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 2103 to REG_DWORD = 3.

Group ID (Vulid): V-22635

Group Title: DTBI920: Run .NET Framework-reliant components not

Rule ID: SV-26382r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI920

Rule Title: Run .NET Framework-reliant components not signed with Authenticode (Internet Zone) property is not properly set.

Vulnerability Discussion: This policy setting allows you to manage whether .NET Framework components that are not signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone “Run .NET Framework-reliant components not signed with Authenticode” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 2004 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone “Run .NET Framework-reliant components not signed with Authenticode” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 2004 to REG_DWORD = 3.

Group ID (Vulid): V-22636

Group Title: DTBI930: Run .NET Framework-reliant components sig

Rule ID: SV-26386r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI930

Rule Title: Run .NET Framework-reliant components signed with Authenticode (Internet Zone) property is not properly set.

Vulnerability Discussion: This policy setting allows you to manage whether .NET Framework components that are signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone “Run .NET Framework-reliant components signed with Authenticode” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: If the value 2001 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone “Run .NET Framework-reliant components signed with Authenticode” will be set to “Enabled” and “Disable”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Criteria: Set the value 2001 to REG_DWORD = 3.

Group ID (Vulid): V-22637

Group Title: DTBI940: Allow Scriptlets

Rule ID: SV-26389r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI940

Rule Title: Allow Scriptlets (Restricted Sites Zone) property is not properly set.

Vulnerability Discussion: This policy setting allows you to manage whether scriptlets can be allowed.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone “Allow Scriptlets” will be set to “Enabled” and “Disabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 1209 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone “Allow Scriptlets” will be set to “Enabled” and “Disabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1209 to REG_DWORD = 3.

Group ID (Vulid): V-22638

Group Title: DTBI950: Allow status bar updates via script

Rule ID: SV-26392r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI950

Rule Title: Allow status bar updates via script (Restricted Sites Zone) property is not properly set.

Vulnerability Discussion: This policy setting allows you to manage whether script is allowed to update the status bar within the zone.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone "Allow status bar updates via script" will be set to "Enabled" and "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: If the value 2103 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone "Allow status bar updates via script" will be set to "Enabled" and "Disabled". Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 2103 to REG_DWORD = 3.

Group ID (Vulid): V-22687

Group Title: DTBI1010: IE Processes Restrict ActiveX Install

Rule ID: SV-27076r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI1010

Rule Title: Internet Explorer Processes Restrict ActiveX Install (Explorer) property is not properly set.

Vulnerability Discussion: This policy setting enables blocking of ActiveX control installation prompts for Internet Explorer processes. If you do not configure this policy setting, the user's preference will be used to determine whether to block ActiveX control installations for Internet Explorer processes.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict ActiveX Install -> "Internet Explorer Processes" will be set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict ActiveX Install -> "Internet Explorer Processes" will be set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-22688

Group Title: DTBI1020: IE Processes Restrict ActiveX Install

Rule ID: SV-27078r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTBI1020

Rule Title: Internet Explorer Processes Restrict ActiveX Install (IExplorer) property is not properly set.

Vulnerability Discussion: This policy setting enables blocking of ActiveX control installation prompts for Internet Explorer processes. If you do not configure this policy setting, the user's preference will be used to determine

whether to block ActiveX control installations for Internet Explorer processes.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict ActiveX Install -> "Internet Explorer Processes" will be set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL Criteria: If the value iexplorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict ActiveX Install -> "Internet Explorer Processes" will be set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL Criteria: Set the value iexplorer.exe to REG_SZ = 1.

UNCLASSIFIED